Zadanie realizowane jest w zakresie umowy o powierzenie grantu o numerze **FERC.02.02-CS.01-001/23/1371/ FERC.02.02-CS.01-001/23/2024** w ramach konkursu grantowego w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23
Zadanie ,,Cyberbezpieczny samorząd” finansowany jest ze środków Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC)
Priorytet II: Zaawansowane usługi cyfrowe
Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa

Załącznik – Opis przedmiotu zamówienia

ZP.271.13.2024

Nazwa postępowania: **Zakup i wdrożenie sprzętu komputerowego, oprogramowania na potrzeby projektu "Cyberbezpieczny Samorząd”**

1. **Opis przedmiotu zamówienia:**

Zadanie	Przedmiot zamówienia	Urząd Miejski Ilość (szt.)	M-GOPS Ilość (szt.)
1	Zintegrowany system ochrony sieci klasy UTM wraz z licencją	1	0
2	Zintegrowany system ochrony sieci klasy UTM wraz z licencją	0	1
3	Zintegrowany system do inwentaryzacji	1	0
4	Zintegrowany system do inwentaryzacji	0	1
5	Oprogramowanie antywirusowe	1	0
6	Oprogramowanie antywirusowe	0	1
7	Oprogramowanie DLP (Data Leak Prevention)	1	0
8	Oprogramowanie DLP (Data Leak Prevention)	0	1
9	Serwer do obsługi DLP wraz z peryferiami -zasilacz awaryjny	1	0
10	Serwer do obsługi DLP wraz z peryferiami -zasilacz awaryjny	0	1

11	Rozwiązania kopii bezpieczeństwa w chmurze	1	0
12	Sieciowy serwer plików do archiwizacji danych	1	0
13	Sieciowy serwer plików do archiwizacji danych	0	1
14	Wdrożenie punktów 1-10	1	
15	Wdrożenie punktów 11-13	1	

Licencje i serwis systemów powinny obowiązywać od momentu podpisania umowy przez okres trwania Programu, tj. do 30.06.2026 r.

W celu zbadania poprawności złożonej oferty, Oferent powinien dołączyć karty katalogowe zaoferowanych urządzeń i oprogramowania.

Cena oferty obejmuje także dostawę do Urzędu Miejskiego w Pyzdrach i Miejsko-Gminnego Ośrodka Pomocy Społecznej w Pyzdrach.

2. **Szczegółowy opis przedmiotu zamówienia:**

Lp.	Przedmiot zamówienia
1	Zakup i wdrożenie rozwiązań zawierających funkcjonalności klasy UTM,XDR, DLP, zarządzania podatnościami, monitorowania i inwentaryzacji infrastruktury informatycznej
2	Zakup i wdrożenie kompleksowego rozwiązania w postaci magazynu danych oraz usług chmurowych

1. Zakup i wdrożenie rozwiązań zawierających funkcjonalności klasy UTM, XDR, DLP, zarządzania podatnościami, monitorowania i inwentaryzacji infrastruktury informatycznej.

Szczegółowy opis:

a) Zakup i wdrożenie zintegrowanego systemu ochrony sieci klasy UTM wraz z licencją dla Urzędu Miejskiego i Miejsko - Gminnego Ośrodka Pomocy Społecznej w Pyzdrach. (2 szt.)

OBSŁUGA SIECI

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP i/lub ZAPORA KORPORACYJNA (Firewall).
2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
7. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
10. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
11. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).

12. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

INTRUSION PREVENTION SYSTEM (IPS)

1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
7. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
9. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

KSZTAŁTOWANIE PASMA (Traffic Shapping)

1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

OCHRONA ANTYWIRUSOWA

1. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
4. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

OCHRONA ANTYSPAM

1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
2. Ochrona antyspam ma działać w oparciu o:
   a. białe/czarne listy,
   b. DNS RBL,
   c. Skaner heurystyczny.
3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

WIRTUALNE SIECI PRYWATNE (VPN)

1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
   a. PPTP VPN,
   b. IPSec VPN,
   c. SSL VPN.
3. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).

7. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
8. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

FILTR DOSTĘPU DO STRON WWW

1. Urządzenie ma posiadać wbudowany filtr URL.
2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
3. Administrator ma mieć możliwość dodawania własnych kategorii URL.
4. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
   a. blokowanie dostępu do adresu URL,
   b. zezwolenie na dostęp do adresu URL,
   c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
5. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
6. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
7. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
8. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
9. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
10. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

UWIERZYTELNIANIE

1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
   a. lokalną bazę użytkowników (wewnętrzny LDAP),
   b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
   c. usługę katalogową Microsoft Active Directory.
2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
   a. SSL,
   b. Radius,
   c. Kerberos.

4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
7. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
9. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.

ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
   a. równoważenie względem adresu źródłowego,
   b. równoważenie względem połączenia.
3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
4. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP. ROUTING (TRASOWANIE)
8. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
9. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.

10. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
11. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

ADMINISTRACJA URZĄDZENIEM

1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
6. Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH).
7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
15. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
16. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.

17. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
    a. manualnego eksportu do pliku w dowolnym momencie czasu,
    b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
18. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
19. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
20. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

RAPORTOWANIE

1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

POZOSTAŁE USŁUGI I FUNKCJE

1. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
2. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
3. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.

4. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
5. Urządzenie ma posiadać usługę DNS Proxy.
6. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
7. Urządzenie musi mieć zaimplementowane Open API
8. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
9. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
10. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.

GWARANCJA I SERWIS

1. Urządzenie ma być **objęte 12-miesięczną** gwarancją producenta na dostarczone elementy systemu oraz **licencją dla wszystkich funkcji bezpieczeństwa do końca trwania Programu, tj. 30.06.2026 r.**
2. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

PARAMETRY SPRZĘTOWE

1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash.
2. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
3. Liczba portów Ethernet 2,5Gbps – min. 8.
4. Liczba portów światłowodowych 1Gbps – min. 1.
5. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
6. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
7. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps.
8. Przepustowość filtrowania Antywirusowego – minimum 500Mbps.
9. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.
10. Maksymalna liczba tuneli VPN IPSec – minimum 100.

11. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.
12. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
13. Obsługa interfejsów 802.11q (VLAN) – minimum 128
14. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.
15. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
16. Urządzenie nie ma limitu na liczbę użytkowników.
17. Liczba reguł filtrowania – minimum 8 192.
18. Liczba tras statycznego routingu – minimum 512.
19. Liczba tras dynamicznego routingu – minimum 10 000.
20. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
21. Urządzenie musi być wyposażone w moduł TPM.

b) Zakup i wdrożenie zintegrowanego systemu do inwentaryzacji dla Urzędu Miejskiego w Pyzdrach z serwisem dla 40 użytkowników.

Oprogramowanie ma posiadać budowę modułową, składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami ma być nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. Program ma umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolę zarządzającą. Moduły powinny umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program ma wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji 12) dzięki czemu nie będzie objęty limitem ilości danych, baza danych ma być rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających powinna wymagać 64-bitowego systemu operacyjnego Windows. Dane, które dotyczą działań pracownika na komputerze: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., mają być odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. One powinny być również grupowane w osobnym, dedykowanym oknie. Pozwala to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, ma być objęty kontrolą na poziomie wybranych Administratorów – w programie można będzie nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator powinien mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do opcji programu oraz logów działań innych administratorów. Działania administratorów muszą być logowane oznacza to, że program będzie posiadać dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów będą mogły być automatycznie eksportowane do zewnętrznego kolektora Syslog. System powinien umożliwiać synchronizację kont użytkowników, w tym administratorów z Active Directory, również przez szyfrowane połączenie LDAPS. Program powinien również umożliwiać konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityki muszą pozwalać na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymuszać dostosowanie bieżących haseł do obowiązujących zasad. Program musi zawierać mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji

dwuskładnikowej (MFA). Kod autoryzacyjny może zostać wysyłany za pomocą e-mail i/lub SMS. W weryfikacji MFA możliwe będzie skonfigurowanie okresu, po którym należy ponownie zautoryzować logowanie. W przypadku awarii autoryzacja logowania będzie mogła zostać pominięta tylko w lokalnej konsoli serwera. Producent powinien zostać wyróżniony znakiem jakości CYBERSECURITY MADE IN EUROPE przyznawanym przez Europejską Organizację ds. Cyberbezpieczeństwa (ECSO).

Specyfikacja Techniczna

MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

- wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
- wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)
- wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
- wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
- wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze
- wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
- wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny
- zablokowania mapy urządzeń przed przypadkową edycją
- serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program musi monitorować czas ich odpowiedzi i procent utraconych pakietów serwerów pocztowych:
  - program musi monitorować czas logowania do serwisu odbierającego oraz czas wysyłania poczty
  - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem)
  - program ma możliwość wykonywania operacji testowych
  - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa

- monitorowania serwerów WWW i adresów URL
- cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
- obsługi szyfrowania SSL/TLS w powiadomieniach e-mail
- obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID
- obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
- monitoringu routerów i przełączników wg:
    - zmian stanu interfejsów sieciowych
    - ruchu sieciowego
    - podłączonych stacji roboczych – graficzna prezentacja panelu switcha
    - ruchu generowanego przez podłączone do portów stacje robocze
- serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
- wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
- monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano
- zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny
- wydajności systemów Windows:
    - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy

Program posiada Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć mogą m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program posiada również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP. Program umożliwia również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na

wykryte zdarzenie. Wykonywanie akcji alarmów można skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji można nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00. Alarmy pozwalają na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie umożliwia wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0 Program ma możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

W ZAKRESIE INWENTARYZACJI program automatycznie musi gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

1. Będzie prezentował szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
2. Umożliwiał odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.
3. Obejmował m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
4. Informował o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.
5. Zbierał informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
6. Posiadał możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
7. Umożliwiał odczytanie numeru seryjnego (klucze licencyjne).
8. Umożliwiał automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
9. Umożliwiał przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.
10. Umożliwiał utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
11. Umożliwiał wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji będą logowane. Moduł inwentaryzacji zasobów umożliwiać będzie prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:
    - przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
    - przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów,

- tworzenia powiązań między zasobami a urządzeniami,
- tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
- wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
- definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
- określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
- określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
- masową edycję atrybutów zasobów,
- definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
- importu danych z zewnętrznego źródła (.CSV),
- przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
- tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
- oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
- ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
- generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,
- przygotowania wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
- konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
- konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
- archiwizacji i porównywania audytów zasobów,
- tworzenia kodów kreskowych dla zasobów,
- drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,

- inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
- możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
- inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
- definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data" z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja"). Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:
  - Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
  - Informacje o aplikacjach używanych w organizacji.
  - Tworzenie własnych wzorców aplikacji.
  - Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
  - Informacje o komputerach, na których aplikacja została wykryta.
  - Zarządzanie posiadanymi licencjami.
  - Wskazywanie osób odpowiedzialnych za licencję.
  - Wskazanie użytkowników licencji.
  - Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
  - Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.
  - Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.
  - Zarządzanie posiadanymi licencjami: raport zgodności licencji.
  - Możliwość przypisania do programów numerów seryjnych, wartości itp. Okna audytowe posiadają możliwość filtrowania elementów per oddział.

W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW program musi umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

- Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
- Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,

- Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
- Informacji o edytowanych przez użytkownika dokumentach,
- Historii pracy (cykliczne zrzuty ekranowe),
- Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),
- Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
- Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków, nagłówków przesyłanej w aplikacjach klienckich poczty e-mail.

Program ponadto posiada możliwość:

- wykrywania podejrzanej aktywności przez popularne „jigglery", mającej na celu symulowanie faktycznej pracy.
- zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury.
- wyszczególnienia podejrzanej aktywności w raportach.
- wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności.
- automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności.
- blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami.
- integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT.
- skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia.
- automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych.
- blokowania ruchu na wskazanych portach TCP/IP,
- blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
- prowadzenia rejestru naruszeń blokad,

- wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,
- przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
- definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. Program posiada Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

PROGRAM MUSI UMOŻLIWIAĆ REALIZACJĘ ZDALNEJ POMOCY UŻYTKOWNIKOM. W ramach kontroli stacji użytkownika musi być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator muszą widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu musi mieć możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu musi umożliwiać równoczesne podłączenie do tego samego komputera kilku administratorom. W module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie musi pozwalać na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł musi umożliwiać również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawierać dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Program musi umożliwiać użytkownikom monitorowanie procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. System musi umożliwiać użycie pośredniego statusu „zgłoszenie rozwiązane” przed ostatecznym zamknięciem zgłoszenia. Moduł musi zawierać również komunikator (czat), który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i

administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów). Ponadto czat musi pozwalać na:

- zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej
- rozmowy również między „zwykłymi" użytkownikami
- przesyłanie plików między rozmówcami w trybie online
- tworzenie pokojów tematycznych, rozmów grupowych
- oznaczanie kontaktów jako „ulubionych" na liście kontaktów
- uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW helpdesku
- może być wyświetlany w trybie jasnym lub ciemnym. W module zawarta powinna być baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program musi umożliwiać informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Użytkownik musi mieć możliwość przeglądania historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. Administrator musi mieć możliwość tworzenia szkiców i archiwizowania komunikatów. Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany musi być przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.

Funkcjonalność modułu musi umożliwiać również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika. Moduł pomocy zdalnej będzie umożliwiać również:

- pobieranie listy użytkowników z Active Directory,
- wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym,
- zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,
- zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
- zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń,
- zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy,
- tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,
- automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,

  - definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,
  - przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,
  - procesowanie zgłoszeń użytkowników z wiadomości e-mail,
  - eksportowania listy zgłoszeń do plików CSV i XLSX,
  - integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0,
- tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
- wykonywanie operacji na wielu zgłoszeniach równocześnie,
- dołączanie załączników do zgłoszeń,
- rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,
- szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
- wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
- zrzuty ekranowe (podgląd pulpitu),
- zdalną modyfikację rejestrów,
- dystrybucję oprogramowania przez Agenty,
- definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami,
- przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników,
- dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),
- zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,
- możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,
- możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy,
- planowanie nieobecności pracowników helpdesk,
- obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,
- generowanie raportów obsługi helpdesk,
- zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),
- zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),

- wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.

Oprogramowanie musi mieć MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM poprzez blokowanie urządzeń.

1. Blokowanie urządzeń i nośników danych. Program musi mieć możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
8. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.
9. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.
10. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
11. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.
12. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

Zarządzanie prawami dostępu do urządzeń:

1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.
3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

Audyt operacji na plikach na urządzeniach przenośnych:

1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.

2. Podłączenie/odłączenie urządzenia przenośnego. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. Definiowanie reguł monitorowanych folderów w postaci list. Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.) Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych. Program umożliwia prowadzenie rejestru naruszeń blokad podłączanych nośników.

Program musi WSPIERAĆ ZARZĄDZANIE CZASEM I ANALIZOWANIE AKTYWNOŚCI UŻYTKOWNIKÓW poprzez dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji powinien oznaczyć sesję aktywności jako czas prywatny gdy wykonuje czynności prywatne na sprzęcie firmowym. Powinien również uzyskać dostęp do własnych wskaźników aktywności w czasie pracy. Menedżerowie oraz przełożeni będą mogli uzyskać automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz będą mogli przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Pracownik będzie mógł przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. Zastosowane reguły pozwalają zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. Dostęp realizowany powinien przez przeglądarkę internetową a strona wyświetlana w trybie jasnym lub ciemnym.

1. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.
2. Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.
3. Statystyki aktywności podwładnych widoczne dla przełożonego.
4. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.
5. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.
6. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.
7. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.
8. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.
9. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy.
10. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).
11. Wskaźnik czasu poświęconego na aktywność produktywną.

12. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.
13. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z możliwością edycji.
14. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.

Oprogramowanie musi posiadać również obszar funkcjonalny w formie platformy WWW, który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami, których nazwy można zmieniać wg potrzeb. Na każdym z dashboardów widgety są rozłożone na siatce o rozmiarze ustalonym przez administratora. Zawartość każdego z paneli informacyjnych ma być automatycznie odświeżana oraz może być:

- Udostępniana w trybie „tylko do odczytu" z zabezpieczeniem tokenem.
- Wyświetlana w trybie jasnym lub ciemnym (nocnym). Oprogramowanie umożliwia zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego. Widgety prezentują dane ze wszystkich modułów funkcjonalnych oprogramowania:
    - Mapa sieci,
    - Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci,
    - Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów,
    - Statystyki z obszaru wydruków, Statystki użycia aplikacji, Użycie łącza, Aktywność WWW, naruszenia reguł blokad,
    - Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie,
    - Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem), informacje o stanie Bitlocker, Windows Defender, Windows Firewall, naruszenia reguł dostępu do nośników danych,
    - Produktywność dla grupy, Statystyki czasu nieproduktywnego.

Ochrona przed usunięciem

Program powinien być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.

Funkcjonalność Agenta

Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.

Inne

Globalna wyszukiwarka, zwracająca wyniki obiektów różnego typu na podstawie wyszukiwanych słów kluczowych, np.: urządzenia, użytkownicy, zasoby, elementy interfejsu konsoli zarządzającej, elementy opcji. Program dostępny jest w języku polskim, angielskim, bułgarskim i litewskim, wraz z Podręcznikiem Użytkownika w formie strony internetowej.

c) **Zakup i wdrożenie zintegrowanego systemu do inwentaryzacji dla Miejsko - Gminnego Ośrodka Pomocy Społecznej w Pyzdrach z serwisem dla 20 użytkowników.**

Oprogramowanie musi posiadać budowę modułową, składać się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana jest przy użyciu szyfrowanego protokołu TLS 1.2. Program ma umożliwiać zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą. Moduły mają umożliwiać kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program powinien wykorzystywać darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji 12) dzięki czemu nie jest objęty limitem ilości danych, baza danych ma być rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających powinna wymagać 64-bitowego systemu operacyjnego Windows. Dane, które dotyczą działań pracownika na komputerze: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., powinny zostać odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Mają być również grupowane w osobnym, dedykowanym oknie. Pozwala to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej. Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, powinien zostać objęty kontrolą na poziomie wybranych Administratorów – w programie powinna być możliwość nadawania kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator ma mieć możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Działania administratorów powinny być logowane oznacza to, że program posiadać powinien dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów powinny być

automatycznie eksportowane do zewnętrznego kolektora Syslog. Lista kont użytkowników, w tym administratorów, powinna być synchronizowana z Active Directory, również przez szyfrowane połączenie LDAPS. Program ma umożliwiać konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityki powinny pozwalać na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymuszać dostosowanie bieżących haseł do obowiązujących zasad. Program zawierać powinien mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny powinien zostać wysyłany za pomocą e-mail i/lub SMS. W weryfikacji MFA można będzie skonfigurować okres, po którym należy ponownie zautoryzować logowanie. W przypadku awarii autoryzacja logowania będzie mogła zostać pominięta tylko w lokalnej konsoli serwera. Producent powinien zostać wyróżniony znakiem jakości CYBERSECURITY MADE IN EUROPE przyznawanym przez Europejską Organizację ds. Cyberbezpieczeństwa (ECSO).

Specyfikacja Techniczna

MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) obejmować powinno serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:

- wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping
- wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU)
- wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci
- wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła.
- wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku
- wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze
- wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie
- wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny
- zablokowania mapy urządzeń przed przypadkową edycją
- serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów
- serwerów pocztowych:
    - program powinien monitorować czas logowania do serwisu odbierającego oraz czas wysyłania poczty

  - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem)
  - program ma możliwość wykonywania operacji testowych
  - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa
- monitorowania serwerów WWW i adresów URL
- cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS
- obsługi szyfrowania SSL/TLS w powiadomieniach e-mail
- obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID
- obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych
- monitoringu routerów i przełączników wg:
  - zmian stanu interfejsów sieciowych
  - ruchu sieciowego
  - podłączonych stacji roboczych – graficzna prezentacja panelu switcha
  - ruchu generowanego przez podłączone do portów stacje robocze
- serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie
- wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu
- monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano
- zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny
- wydajności systemów Windows:
  - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy Program ma posiadać Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć powinny m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program ma posiadać również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP. Program ma umożliwia również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami

w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów można skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji można nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00. Alarmy pozwalają na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie umożliwia wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0 Program ma możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).

W ZAKRESIE INWENTARYZACJI program automatycznie powinien gromadzić informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:

1. Prezentować szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.
2. Umożliwiać odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.
3. Obejmować m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.
4. Informować o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikować użytkowania licencji w organizacji.
5. Zbierać informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.
6. Posiadać możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.
7. Umożliwiać odczytanie numeru seryjnego (klucze licencyjne).
8. Umożliwiać automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.
9. Umożliwiać przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.

10. Umożliwiać utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).
11. Umożliwiać wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji powinny być logowane. Moduł inwentaryzacji zasobów umożliwiać powinien prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:
    - przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji,
    - przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów,
    - tworzenia powiązań między zasobami a urządzeniami,
    - tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,
    - wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy,
    - definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz,
    - określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów,
    - określenia atrybutów dodatkowych tylko dla wybranych typów zasobów,
    - masową edycję atrybutów zasobów,
    - definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie,
    - importu danych z zewnętrznego źródła (.CSV),
    - przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp.,
    - tworzenia powiązań między zasobami a dokumentami w relacji 1:N,
    - oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp.,
    - ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności,
    - generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania,

- przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji,
- konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca,
- konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca,
- archiwizacji i porównywania audytów zasobów,
- tworzenia kodów kreskowych dla zasobów,
- drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy,
- inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet,
- możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android,
- inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline),
- definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).

  Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:
  - Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.
  - Informacje o aplikacjach używanych w organizacji.
  - Tworzenie własnych wzorców aplikacji.
  - Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.
  - Informacje o komputerach, na których aplikacja została wykryta.
  - Zarządzanie posiadanymi licencjami.
  - Wskazywanie osób odpowiedzialnych za licencję.
  - Wskazanie użytkowników licencji.
  - Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.
  - Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.

- Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.
- Zarządzanie posiadanymi licencjami: raport zgodności licencji.
- Możliwość przypisania do programów numerów seryjnych, wartości itp. Okna audytowe posiadają możliwość filtrowania elementów per oddział.

W ZAKRESIE OBSŁUGI UŻYTKOWNIKÓW program ma umożliwiać monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:

- Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy),
- Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach,
- Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność,
- Informacji o edytowanych przez użytkownika dokumentach,
- Historii pracy (cykliczne zrzuty ekranowe),
- Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt),
- Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika),
- Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków,
- Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail. Program ponadto posiada możliwość:
  - wykrywania podejrzanej aktywności przez popularne „jigglery”, mającej na celu symulowanie faktycznej pracy.
  - zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury.
  - wyszczególnienia podejrzanej aktywności w raportach.
  - wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności.
  - automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności.

- blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami.
- integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT.
- skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia.
- automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych.
- blokowania ruchu na wskazanych portach TCP/IP,
- blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem,
- prowadzenia rejestru naruszeń blokad,
- wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady,
- przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika),
- definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami. Program posiada Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.

PROGRAM UMOŻLIWIAĆ POWINIEN REALIZACJĘ ZDALNEJ POMOCY UŻYTKOWNIKOM. W ramach kontroli stacji użytkownika ma być dostępny podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator powinni widzieć ten sam ekran. Administrator w trakcie zdalnego dostępu ma mieć możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu ma umożliwiać będzie równoczesne podłączenie do tego samego komputera kilku administratorom. W module powinna znajdować się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim administratorom,

otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie powinno pozwalać na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł umożliwiać powinien również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach") oraz zawierać dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. System umożliwiać będzie użycie pośredniego statusu „zgłoszenie rozwiązane" przed ostatecznym zamknięciem zgłoszenia. Moduł powinien również zawierać komunikator (czat), który umożliwiałby prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów). Ponadto czat powinien pozwalać na:

- zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej
- rozmowy również między „zwykłymi" użytkownikami
- przesyłanie plików między rozmówcami w trybie online
- tworzenie pokojów tematycznych, rozmów grupowych
- oznaczanie kontaktów jako „ulubionych" na liście kontaktów
- uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku
- może być wyświetlany w trybie jasnym lub ciemnym.

  W module powinna być zawarta również baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program ma umożliwiać informowania pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Użytkownik powinien mieć możliwość przeglądania historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. Administrator miałby możliwość tworzenia szkiców i archiwizowania komunikatów. Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany będzie przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.

Funkcjonalność modułu umożliwia również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika. Moduł pomocy zdalnej umożliwia również:

- pobieranie listy użytkowników z Active Directory,
- wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym,
- zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont,
- zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń,
- zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń,
- zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy,
- tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,
- automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników,
- definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji,
- przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii,
- procesowanie zgłoszeń użytkowników z wiadomości e-mail,
- eksportowania listy zgłoszeń do plików CSV i XLSX,
- integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0,
- tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń,
- wykonywanie operacji na wielu zgłoszeniach równocześnie,
- dołączanie załączników do zgłoszeń,
- rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy,
- szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników,
- wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia,
- zrzuty ekranowe (podgląd pulpitu),
- zdalną modyfikację rejestrów,
- dystrybucję oprogramowania przez Agenty,
- definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami,
- przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników,
- dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI),

- zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku,
- możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu,
- możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy,
- planowanie nieobecności pracowników helpdesk,
- obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem,
- generowanie raportów obsługi helpdesk,
- zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu),
- zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami),
- wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.

Oprogramowanie musi mieć MOŻLIWOŚĆ OCHRONY DANYCH PRZED WYCIEKIEM poprzez blokowanie urządzeń.

1. Blokowanie urządzeń i nośników danych. Program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.
2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.
3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.
4. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.
5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych.
6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.
7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.
8. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.
9. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.

10. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.
11. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.
12. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.

Zarządzanie prawami dostępu do urządzeń:

1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.
2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.
3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.
4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.
5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.

Audyt operacji na plikach na urządzeniach przenośnych:

1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.
2. Podłączenie/odłączenie urządzenia przenośnego. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. Definiowanie reguł monitorowanych folderów w postaci list. Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.) Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych. Program umożliwia prowadzenie rejestru naruszeń blokad podłączanych nośników.

Program ma WSPIERAĆ ZARZĄDZANIE CZASEM I ANALIZOWANIE AKTYWNOŚCI UŻYTKOWNIKÓW poprzez dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji będzie mógł oznaczyć sesję aktywności jako czas prywatny gdy wykonuje czynności prywatne na sprzęcie firmowym. Będzie mógł również uzyskać dostęp do własnych wskaźników aktywności w czasie pracy. Menedżerowie oraz przełożeni będą mogli uzyskać automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz będą mogli przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Pracownik będzie mógł przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. Zastosowane reguły pozwalać będą zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. Dostęp realizowany będzie przez przeglądarkę internetową a strona będzie mogła być wyświetlana w trybie jasnym lub ciemnym.

1. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu.
2. Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy.

3. Statystyki aktywności podwładnych widoczne dla przełożonego. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem.
4. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu.
5. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników.
6. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych.
7. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne.
8. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy.
9. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie).
10. Wskaźnik czasu poświęconego na aktywność produktywną.
11. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail.
12. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z możliwością edycji.
13. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.

Oprogramowanie posiadać będzie również obszar funkcjonalny w formie platformy WWW, który będzie pozwalać na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami, których nazwy można będzie zmieniać wg potrzeb. Na każdym z dashboardów widgety będą rozłożone na siatce o rozmiarze ustalonym przez administratora. Zawartość każdego z paneli informacyjnych jest automatycznie odświeżana oraz może być:

- Udostępniana w trybie „tylko do odczytu” z zabezpieczeniem tokenem.
- Wyświetlana w trybie jasnym lub ciemnym (nocnym). Oprogramowanie umożliwiać będzie zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego. Widgety powinny prezentują dane ze wszystkich modułów funkcjonalnych oprogramowania:
  - Mapa sieci,
  - Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci,
  - Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów,
  - Statystyki z obszaru wydruków, Statystki użycia aplikacji, Użycie łącza, Aktywność WWW, naruszenia reguł blokad,

- Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie,
- Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem), informacje o stanie Bitlocker, Windows Defender, Windows Firewall, naruszenia reguł dostępu do nośników danych,
- Produktywność dla grupy, Statystyki czasu nieproduktywnego.

Ochrona przed usunięciem

Program powinien być zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.

Funkcjonalność Agenta

Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.

Inne

Globalna wyszukiwarka, zwracająca wyniki obiektów różnego typu na podstawie wyszukiwanych słów kluczowych, np.: urządzenia, użytkownicy, zasoby, elementy interfejsu konsoli zarządzającej, elementy opcji. Program dostępny jest w języku polskim, angielskim, bułgarskim i litewskim, wraz z Podręcznikiem Użytkownika w formie strony internetowej.

d) Zakup i wdrożenie oprogramowania antywirusowego dla Urzędu Miejskiego w Pyzdrach z serwisem dla 40 użytkowników

Specyfikacja techniczna:

Administracja zdalna w chmurze

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.

7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.

11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.

19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
    - tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
    - tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
    - tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
24. Rozwiązanie musi być wyposażone w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie, do celów skanowania plików na macierzach NAS/SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów.

Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
   a. usunięcie zawartości urządzenia,
   b. przywrócenie urządzenie do ustawień fabrycznych, c. zablokowania urządzenia,
   c. uruchomienie sygnału dźwiękowego,
   d. lokalizację GPS.

6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
   a. nazwę aplikacji,
   b. nazwę pakietu,
   c. kategorię sklepu Google Play,
   d. uprawnienia aplikacji,
   e. pochodzenie aplikacji z nieznanego źródła.

Ochrona serwera pocztowego MS Exchange

1. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych.
2. Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019.
3. Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
4. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
5. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
6. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
7. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
8. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
9. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
10. Rozwiązanie ma posiadać mechanizm greylisting (szara lista).
11. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
    a. Czysty,
    b. Podejrzany,
    c. Bardzo podejrzany,
    d. Szkodliwy.
13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

Ochrona usługi Microsoft 365

1. Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams.
2. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Micosoft 365.
3. Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.
4. Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.
5. Rozwiązanie musi być dostępny w języku polskim.
6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej: a) użytkowników, otrzymujących najwięcej spamu, b) użytkowników, otrzymujących najwięcej wiadomości typu „phishing", c) użytkowników, otrzymujących największą ilość szkodliwego oprogramowania, d) kont użytkowników, które mogę być podejrzane.
7. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.
8. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej:
   a. jaka ilość wiadomości została przeskanowania,
   b. wynik skanowania poszczególnej wiadomości,
   c. czynność podjęta przez rozwiązanie.
9. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o:
   a. zagrożeniach, które zostały wykryte,
   b. na jakim koncie zostały wykryte,
   c. jakie zagrożenie zostało wykryte,
   d. podjętą czynność.
10. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.
11. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.
12. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.
13. Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej:
   a. wykorzystania do analizy mechanizmów chmurowych, tego samego producenta,
   b. wprowadzenia białych i czarnych list adresów ochrony Exchange'a Online,
   c. dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.
14. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.

15. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.
16. Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
17. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
18. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.

Moduł XDR

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.

12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia.

Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.

1. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
2. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
3. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
4. Konsola administracyjna musi mieć możliwość tagowania obiektów.
5. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

Moduł zarządzania podatnościami i aktualizacjami

1. Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.
2. Baza wykrywanych podatności musi zawierać minimum 35000 CVE.
3. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli, ani innych dodatkowych komponentów na stacjach końcowych.
4. Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie.
5. Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum:
   - nazwę aplikacji lub systemu operacyjnego
   - punktacje CVSS

- opis wykrytej podatności
- wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta

6. Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.
7. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
8. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
9. Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
10. Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
11. Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.
12. Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.
13. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.
14. Moduł wykrywania podatności powinien wykrywać podatności w minimum 700 aplikacjach.

Ochrona poprzez dwuskładnikowe uwierzytelnianie

1. Rozwiązanie musi wspierać systemy operacyjne Microsoft Windows Server: 2008 / 2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials / Windows Server 2022.
2. Rozwiązanie musi wspierać system operacyjne Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11.
3. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.

4. Oprogramowanie musi wspierać integrację z Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019.
5. Oprogramowanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016.
6. Oprogramowanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 / 2019.
7. Oprogramowanie musi wspierać integrację z Microsoft Remote Desktop Web Access.
8. Oprogramowanie musi wspierać integrację z Microsoft Terminal Services Web Access.
9. Oprogramowanie musi wspierać integrację z Microsoft Remote Web Access.
10. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.
11. Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej).
12. Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji.
13. Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.
14. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.
15. Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS.
16. Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego
17. Wsparcie techniczne do programu świadczone w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta programu.

e) Zakup i wdrożenie oprogramowania antywirusowego dla Miejsko - Gminnego Ośrodka Pomocy Społecznej w Pyzdrach z dla 20 użytkowników

Specyfikacja techniczna:

Administracja zdalna w chmurze

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.

4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu http Proxy.
6. Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
8. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
9. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
10. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
11. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
12. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.

8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    - tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    - tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

17. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
    - tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    - tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
    - tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
    - tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
24. Rozwiązanie musi być wyposażone w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
26. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
27. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
28. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
29. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

30. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL), Rocky Linux, Ubuntu, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows:

1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych .
8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
4. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów.

Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.

3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
   a. usunięcie zawartości urządzenia,
   b. przywrócenie urządzenie do ustawień fabrycznych, c. zablokowania urządzenia,
   c. uruchomienie sygnału dźwiękowego,
   d. lokalizację GPS.
6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: a. nazwę aplikacji,
   a. nazwę pakietu,
   b. kategorię sklepu Google Play,
   c. uprawnienia aplikacji,
   d. pochodzenie aplikacji z nieznanego źródła.

Ochrona serwera pocztowego MS Exchange

1. Rozwiązanie musi wspierać instalację na systemach Microsoft Windows Server 2012 i nowszych.
2. Rozwiązanie musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2010/2013/2016/2019.
3. Rozwiązanie musi zapewniać wsparcie dla ról Mailbox, Edge, Hub.
4. Rozwiązanie musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
5. Rozwiązanie musi zapewnić skanowanie bezpośrednio w bazach danych Exchange przy pomocy VSAPI.
6. Rozwiązanie musi mieć możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
7. Rozwiązanie musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
8. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.

9. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL, z których będzie korzystać aplikacja.
10. Rozwiązanie ma posiadać mechanizm greylisting (szara lista).
11. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
    a. Czysty,
    b. Podejrzany,
    c. Bardzo podejrzany,
    d. Szkodliwy.
13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

Ochrona usługi Microsoft 365

1. Rozwiązanie musi obejmować ochroną usługi Microsoft, takie jak Exchange Online, Onedrive, Sharepoint oraz aplikację Teams.
2. Rozwiązanie musi posiadać możliwość dodania kilku tenantów usługi Micosoft 365.
3. Administrator musi mieć możliwość wskazania, które konto użytkownika będzie objęte ochroną.
4. Rozwiązanie musi być zarządzane za pomocą dowolnej przeglądarki internetowej z dowolnego miejsca w sieci.
5. Rozwiązanie musi być dostępny w języku polskim.
6. Konsola rozwiązania musi posiadać możliwość raportowania co najmniej:
   a. użytkowników, otrzymujących najwięcej spamu,
   b. użytkowników, otrzymujących najwięcej wiadomości typu „phishing”,
   c. użytkowników, otrzymujących największą ilość szkodliwego oprogramowania,
   d. kont użytkowników, które mogę być podejrzane.
7. Konsola rozwiązania musi posiadać funkcjonalność logowania zdarzeń z podziałem na dzienniki dla Exchange Online i Onedrive.
8. Dzienniki Exchange Online muszą posiadać funkcjonalność informowania co najmniej:
   a. jaka ilość wiadomości została przeskanowania,
   b. wynik skanowania poszczególnej wiadomości,
   c. czynność podjęta przez rozwiązanie.
9. Dzienniki Onedrive muszą posiadać funkcjonalność informowania co najmniej o:
   a. zagrożeniach, które zostały wykryte,
   b. na jakim koncie zostały wykryte,
   c. jakie zagrożenie zostało wykryte,
   d. podjętą czynność.
10. Rozwiązanie musi posiadać funkcjonalność kwarantanny, do której będą przenoszone zainfekowane obiekty z usługi Exchange Online oraz Onedrive.
11. Musi istnieć możliwość pobrania plików z kwarantanny w formie oryginalnego pliku i pliku zabezpieczonego hasłem.
12. Administrator musi posiadać możliwość przypisania konfiguracji, do dodanych do rozwiązania tenantów lub do poszczególnych grup i użytkowników.

13. Administrator musi posiadać możliwość konfiguracji rozwiązania w oparciu o co najmniej:
    a. wykorzystania do analizy mechanizmów chmurowych, tego samego producenta,
    b. wprowadzenia białych i czarnych list adresów ochrony Exchange'a Online,
    c. dodania znacznika do tematu wiadomości zakwalifikowanej jako SPAM i phishing.
14. Rozwiązanie musi zapewniać funkcję ochrony przed zagrożeniami 0-day.
15. Funkcja ochrony przed zagrożeniami 0-day musi wykorzystywać do działania chmurę producenta.
16. Funkcja ochrony przed zagrożeniami 0-day musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
17. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
18. Rozwiązanie musi posiadać możliwość przesyłania powiadomień e-mail z funkcją wyboru preferowanego języka.

Moduł XDR

1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica".
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.

10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia.

Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.

1. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
2. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
3. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
4. Konsola administracyjna musi mieć możliwość tagowania obiektów.
5. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.

Moduł zarządzania podatnościami i aktualizacjami

1. Rozwiązanie musi mieć możliwości wykrywania podatności w systemach operacyjnych (co najmniej Windows 10, Windows 11) oraz aplikacjach zainstalowanych na zarządzanych stacjach.
2. Baza wykrywanych podatności musi zawierać minimum 35000 CVE.

3. Rozwiązanie nie może wymagać instalacji dodatkowej konsoli, ani innych dodatkowych komponentów na stacjach końcowych.
4. Automatyczne wykrywanie podatności musi wykonywać się zgodnie z harmonogramem, nie częściej niż raz dziennie.
5. Moduł wykrywania podatności musi umożliwiać wyświetlanie szczegółów danej podatności zawierające minimum:
   - nazwę aplikacji lub systemu operacyjnego
   - punktacje CVSS
   - opis wykrytej podatności
   - wartość ryzyka oceniona przez wewnętrzne mechanizmy producenta
6. Moduł wykrywania podatności musi wykrywać podatności w minimum 700 aplikacjach.
7. Moduł zarządzania aktualizacjami musi umożliwiać wykonanie automatycznej aktualizacji dla minimum 150 popularnych aplikacji.
8. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie białej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje będą aplikowane tylko i wyłącznie dla wskazanych aplikacji w białej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
9. Moduł zarządzania aktualizacjami musi umożliwiać stworzenie czarnej listy aplikacji podlegających automatycznej aktualizacji. Automatyczne aktualizacje oprogramowania będą realizowane dla wszystkich - ponad 150 aplikacji, oprócz aplikacji wskazanych na czarnej liście. Wybór aplikacji musi być możliwy z poziomu listy przygotowanej przez producenta rozwiązania.
10. Zarządzanie aktualizacjami aplikacji musi umożliwiać ręczne wdrażanie poprawek na wybranych stacjach.
11. Moduł zarządzania aktualizacjami oraz wykrywania podatności musi być zintegrowany bezpośrednio z programem antywirusowym tego samego producenta zainstalowanym na zarządzanym komputerze.
12. Stacja robocza posiadająca włączony moduł wykrywania podatności oraz zarządzania aktualizacjami musi być w odpowiedni sposób oznaczona w konsoli centralnego zarządzania.
13. Administrator konsoli musi mieć możliwość włączenia modułu wykrywania podatności i zarządzania aktualizacjami przy pomocy menu kontekstowego dostępnego w konsoli centralnego zarządzania.
14. Moduł wykrywania podatności ma umożliwiać wyłączenie powiadomień dla wybranej podatności.

Ochrona poprzez dwuskładnikowe uwierzytelnianie :

1. Rozwiązanie musi wspierać systemy operacyjne Microsoft Windows Server: 2008 / 2008 R2 / 2012 / 2012 R2 / SBS 2008 / SBS 2011 / 2012 Essentials / 2012 R2 Essentials / Windows Server 2016 / Windows Server 2016 Essentials / Windows Server 2019 / Windows Server 2019 Essentials / Windows Server 2022.
2. Rozwiązanie musi wspierać system operacyjne Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11.
3. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
4. Oprogramowanie musi wspierać integrację z Microsoft Exchange 2007 / 2010 / 2013 / 2016 / 2019.
5. Oprogramowanie musi wspierać integrację z Microsoft Dynamics CRM 2011 / 2013 / 2015 / 2016.
6. Oprogramowanie musi wspierać integrację z Microsoft Sharepoint 2010 / 2013 / 2016 / 2019.
7. Oprogramowanie musi wspierać integrację z Microsoft Remote Desktop Web Access.
8. Oprogramowanie musi wspierać integrację z Microsoft Terminal Services Web Access.
9. Oprogramowanie musi wspierać integrację z Microsoft Remote Web Access.
10. Rozwiązanie musi posiadać wbudowany serwer RADIUS umożliwiający uwierzytelnianie użytkowników dla rozwiązań VPN, które wspierają protokół RADIUS.
11. Aplikacja mobilna musi wspierać telefony działające pod kontrolą systemów mobilnych: Android (w wersji 4.4 lub wyższej), iOS (12 lub wyższej).
12. Aplikacja mobilna do generowania OTP (jednorazowego hasła) musi być dostarczona przez producenta rozwiązania w ramach zakupionej licencji.
13. Użytkownik musi mieć możliwość dodatkowego zabezpieczenia aplikacji w postaci kodu PIN.
14. Aplikacja do działania nie może wymagać od użytkownika aktywnego połączenia z Internetem – generowanie OTP (jednorazowego hasła) musi odbywać się w trybie offline.
15. Dwuskładnikowe uwierzytelnienie musi być możliwe również przy użyciu jednorazowych haseł SMS.
16. Aplikacja zainstalowana na urządzeniach mobilnych musi umożliwiać generowanie OTP dla więcej niż jednego serwera uwierzytelniającego 17. Wsparcie techniczne do programu świadczone w języku polskim, przez polskiego dystrybutora autoryzowanego przez producenta programu

f) **Zakup i wdrożenie oprogramowania DLP (Data Leak Prevention), którego zadaniem jest ochrona danych przed kradzieżą i wyciekami, zarówno przypadkowymi, jak i celowymi dla Urzędu Miejskiego w Pyzdrach z serwisem dla 40 użytkowników.**

Wymagania oprogramowania:

1. System operacyjny:
   a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
   b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
   c. MacOS 12 lub nowszy.
2. Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016 (64-bit) i nowszych.
3. Serwer administracyjny musi obsługiwać bazy danych:
   a. MS SQL Server 2016 lub nowsze,
   b. MS SQL Express,
   c. AzureSQL S3 lub nowsze.
4. Pomoc i dokumentacja programu dostępne w języku angielskim.
5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.
8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
11. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.
12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.
14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.

17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.
19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
20. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
22. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
23. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.
24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.
25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
26. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.
27. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.
28. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
29. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
30. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
31. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
32. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.

33. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
34. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach
35. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.)
36. System musi zapewniać możliwość zarządzanie szyfrowaniem dysków twardych oraz urządzeń wymiennych.

g) Zakup i wdrożenie oprogramowania DLP (Data Leak Prevention), którego zadaniem jest ochrona danych przed kradzieżą i wyciekami, zarówno przypadkowymi, jak i celowymi dla Miejsko - Gminnego Ośrodka Pomocy Społecznej w Pyzdrach z serwisem dla 20 użytkowników.

Wymagania oprogramowania:

1. System operacyjny:
   a. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
   b. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
   c. MacOS 12 lub nowszy.
2. Serwer administracyjny musi obsługiwać instalację na systemach: a. Windows Server 2016 (64-bit) i nowszych.
3. Serwer administracyjny musi obsługiwać bazy danych:
   a. MS SQL Server 2016 lub nowsze,
   b. MS SQL Express,
   c. AzureSQL S3 lub nowsze.
4. Pomoc i dokumentacja programu dostępne w języku angielskim.
5. Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
6. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
7. Serwer administracyjny musi umożliwiać instalację/dezinstalację zdalnego klienta na stacjach roboczych.
8. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
9. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
10. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
11. System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.

12. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
13. Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.
14. Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
15. Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
16. Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
17. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
18. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.
19. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
20. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
21. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
22. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
23. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.
24. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.
25. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
26. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.
27. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu

osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.

28. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
29. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
30. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
31. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
32. System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników Microsoft 365.
33. System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
34. System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach
35. System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.)
36. System musi zapewniać możliwość zarządzanie szyfrowaniem dysków twardych oraz urządzeń wymiennych.

h) Zakup serwera do obsługi DLP, oprogramowania antywirusowego oraz inwentaryzacyjnego wraz z peryferiami tj. zasilacz awaryjny dla Urzędu Miejskiego w Pyzdrach.

Serwer - 1 szt.

Specyfikacja techniczna:

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 2U z możliwością instalacji 12 dysków 3.5” • Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów

	serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 32 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się 16 slotów przeznaczonych do instalacji pamięci. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	• Zainstalowane dwa procesory 8-rdzeniowe, min. 2.9 GHz, Turbo Speed: 4.1 GHz dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 24900 w teście Average CPU Mark Multithread Rating dostępnym na stronie https://www.cpubenchmark.net/.
RAM	• 128GB DDR5 RDIMM 5600MT/s,

Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający
	  ○ Min. 8GB nieulotnej pamięci cache,
	  ○ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
	  ○ Wsparcie dla dysków samoszyfrujących

Dyski twarde	• Zainstalowane: ○ 8 dysków SSD SATA o pojemności min. 960GB, 6Gb, 2,5“ Hot-Plug. • Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Gniazda PCI	• trzy sloty PCIe
Interfejsy sieciowe/FC/SAS	• Wbudowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)

Wbudowane porty	• 4 porty USB w tym min:
	  ○ 1 port USB 3.0 z tyłu obudowy,
	  ○ 1 port micro USB z przodu obudowy
	• 2 port VGA z czego jeden z przodu obudwy
	• Możliwość rozbudowy o port RS232

Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024

Wentylatory	• Redundantne, Hot-Plug
Zasilacze	• Redundantne, Hot-Plug min. 1100W klasy Titanium (1+1)
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
System operacyjny	• System operacyjny Microsoft Windows Server 2022 Standard 64-bit (16 CORE) obsługującego max. 16 rdzeni I 35 licencji dostępowych Win Svr 2022 CAL 1Clt User • W przypadku zaoferowania serwera z liczbą rdzeni przekraczającą standardową licencję dostawca zobowiązany jest do dostarczenia dodatkowych licencji dla Microsoft Windows Serwer 2022 Standard 64-bit w liczbie zapewniającej zgodność z licencjonowaniem Microsoft Windows Serwer Standard 2022 (16 CORE)
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).

Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ○ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; ○ wsparcie dla IPv6; ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ○ integracja z Active Directory; ○ możliwość obsługi przez dwóch administratorów jednocześnie; ○ wsparcie dla automatycznej rejestracji DNS ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.

Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat.
	• Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.
	• Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.
	• Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
	• Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.
	• Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
	• Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.
	• Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
	• Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
	  ○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
	  ○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.

	○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. ○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
Zasilacz UPS do serwera	Moc pozorna: min.3000 VA Moc czynna: min. 2700 W Architektura UPS-a: on-line double conversion Liczba faz na wejściu: 1 (230V) Liczba akumulatorów: 6 Napięcie: min. 12 V Pojemność akumulatora: min. 9 Ah Czas transferu (maks.): 0 ms Czas podtrzymania (obciążenie 100%): min 3 min Czas ładowania: 3 h Typ obudowy: Rack Zabezpieczenia / filtry: Przeciwprzepięciowe Dołączone oprogramowanie: -Możliwość kontrolowania i monitorowania wielu jednostek UPS z sieci lokalnej i internetu -Wykresy analizy mocy, statystyki zdarzeń, eksport historii danych - Wykres danych jednostki UPS w czasie rzeczywistym (napięcie, częstotliwość, poziom obciążenia, poziom naładowania baterii) - Bezpieczne wyłączenie systemu i ochrona danych przed awarią zasilania

	- Powiadomienia za pomocą dźwięków systemowych, e-mail, SMS, do wszystkich komputerów w sieci LAN - Harmonogram włączenia/wyłączenia, test baterii, programowana kontrola gniazda, kontrola alarmów dźwiękowych. - Ochrona dostępu hasłem, dostęp zdalny i zarządzanie - Obsługa wielu języków: Angielski, Chiński, Francuski, Niemiecki, Hiszpański, Rosyjski, Portugalski, Ukraiński, Włoski, Polski, Czeski, Turecki - System operacyjny: Windows/MAC/Linux/Unix/Solaris/AJX/HP-UX/FreeBSD Porty zasilania we.: IEC-C20 Porty zasilania wy: Min. 8 x IEC-C13 Min. 1 x IEC-C19 Gniazda we/wy: Min. 1 x USB (Type B) Min. 1 x RS-232 (COM) Wymagania środowiskowe: - Temperatura operacyjna: 0 - 40 stopni C - Wilgotność otoczenia: 0 - 95% (bez kondensacji) Kolor: Czarny Wymiary: max.438 x max. 608 x max. 86.5 mm Waga: max 28.6 kg

i) Zakup serwera do obsługi DLP, oprogramowania antywirusowego oraz inwentaryzacyjnego wraz z peryferiami tj. zasilacz awaryjny dla Miejsko - Gminnego Ośrodka Pomocy Społecznej w Pyzdrach.

Serwer - 1 szt.
Specyfikacja techniczna:

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 1U z możliwością instalacji do 4 dysków 3.5” • Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

	• Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	• Zainstalowany jeden procesor 4-rdzeniowy, min. 3,4 GHz , Turbo Speed: min 5.0 GHz dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 16540 w teście Average CPU Mark Multithread Rating dostępnym na stronie: https://www.cpubenchmark.net/
Pamięć RAM	• 4x16 GB pamięci RAM DDR5 UDIMM o częstotliwości pracy 5600MT/s.

Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający
	  ○ Min. 8GB nieulotnej pamięci cache,
	  ○ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
	  ○ Wsparcie dla dysków samoszyfrujących

Dyski twarde	• Zainstalowane
	  ○ Zainstalowany 1 dysk HDD SATA o pojemności min. 2TB Hard Drive SATA 6Gbps 7.2K 512n 3.5in Hot-Plug
	  ○ Zainstalowane 2 dyski SSD SATA o pojemności min. 480GB, 6Gb, Hot-Plug.

Sloty PCIe	• Dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT

Wbudowane porty	• min. 4 porty USB w tym min:
	  ○ 1 port USB 3.0 z tyłu obudowy,
	  ○ 1 port micro USB z przodu obudowy
	• 1 port VGA na tylnym panelu,
	• 1 port RS232

Karta graficzna	• Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Zasilacze	• Redundantne, o mocy maks. 700W klasy Titanium
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych

System operacyjny/dodatkowe oprogramowanie	• System operacyjny Microsoft Windows Server 2022 Standard 64-bit (16 CORE) obsługującego max. 16 rdzeni I 30 licencji dostępowych Win Svr 2022 CAL 1Clt User • W przypadku zaoferowania serwera z liczbą rdzeni przekraczającą standardową licencję dostawca zobowiązany jest do dostarczenia dodatkowych licencji dla Microsoft Windows Serwer 2022 Standard 64-bit w liczbie zapewniającej zgodność z licencjonowaniem Microsoft Windows Serwer Standard 2022 (16 CORE)
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 V3 • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).

Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:
	  ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
	  ○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
	  ○ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
	  ○ wsparcie dla IPv6;
	  ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
	  ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;

	○ integracja z Active Directory;; ○ wsparcie dla automatycznej rejestracji DNS ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat.

	• Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.
	• Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.
	• Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
	• Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.
	• Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.
	• Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.
	• Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
	• Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:
	  ○ Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.
	  ○ Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.
	  ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.

	○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
Zasilacz UPS do serwera	Moc pozorna: min.2000 VA Moc czynna: min.1800 W Architektura UPS-a: on-line double conversion Liczba faz na wejściu: 1 (230V) Liczba akumulatorów: 4 Napięcie: 12 V Pojemność akumulatora: min.7 Ah Czas transferu (maks.): 0 ms Czas podtrzymania (obciążenie 100%):min. 3 min Czas ładowania: max. 3 h Typ obudowy : Rack Zabezpieczenia / filtry: Przeciwprzepięciowe Oprogramowanie : -Możliwość kontrolowania i monitorowania wielu jednostek UPS z sieci lokalnej i internetu - Wykresy analizy mocy, statystyki zdarzeń, eksport historii danych - Wykres danych jednostki UPS w czasie rzeczywistym (napięcie, częstotliwość, poziom obciążenia, poziom naładowania baterii)

	- Bezpieczne wyłączenie systemu i ochrona danych przed awarią zasilania - Powiadomienia za pomocą dźwięków systemowych, e-mail, SMS, do wszystkich komputerów w sieci LAN - Harmonogram włączenia/wyłączenia, test baterii, programowana kontrola gniazda, kontrola alarmów dźwiękowych. - Ochrona dostępu hasłem, dostęp zdalny i zarządzanie - Obsługa wielu języków: Angielski, Chiński, Francuski, Niemiecki, Hiszpański, Rosyjski, Portugalski, Ukraiński, Włoski, Polski, Czeski, Turecki - System operacyjny: Windows/MAC/Linux/Unix/Solaris/AJX/HP-UX/FreeBSD Porty zasilania we.: IEC-C14 Porty zasilania wy.: min. 8 x IEC-C13 Gniazda we/wy: Min. 1 x USB (Type B) Min. 1 x RS-232 (COM) Wymagania środowiskowe: -Zalecana temperatura otoczenia: 0 - 40 °C -Zalecana wilgotność otoczenia: 0 - 95 % Akcesoria opcjonalne: Kolor: Czarny Wymiary: max.438 x max.436 x max. 86.5 mm Waga: max. 19.7 kg

2. Zakup i wdrożenie kompleksowego rozwiązania w postaci magazynu danych oraz usług chmurowych

Szczegółowy opis:

a) Zakup i wdrożenie rozwiązania kopii bezpieczeństwa w chmurze dla Urzędu Miejskiego w Pyzdrach

INSTALATOR

Instalator musi umożliwiać zainstalowanie aplikacji klienckiej na komputerze użytkownika końcowego. Na instalator składają się następujące funkcje:

- Kreator instalacji,
- Tłumaczenie instalatora na inne języki,
- Automatyczna instalacja dodatkowych komponentów.

APLIKACJA WINDOWS

Część kliencka musi składać się z dwóch elementów, aplikacji klienckiej oraz usługi systemowej. Aplikacja kliencka instalowana na komputerze użytkownika końcowego odpowiedzialna konfigurację i administrację politykami backupu. Usługa systemowa stanowi właściwy silnik backupu, jest odpowiedzialna za wykonywanie backupów oraz synchronizację danych. Aplikacja kliencka nie musi być uruchomiona dla prawidłowego działania usługi.

Backup i przywracanie danych

- Deduplikacja danych na źródle,
- Backup przyrostowy Delta,
- Backup różnicowy Delta,
- Bare Metal Recovery,
- Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,
- Retencja danych
- Kreator projektów backupów - polityka backupu,
- Projekty backupów,
- Backup danych lokalnych - plikowy,
- Backup MS Outlook,
- Backup MS SQL,
- Backup Firebird,
- Backup dysków sieciowych,
- Backup MS Exchange
- Backup MySQL,

- Backup PostgreSQL,
- Backup System State,
- Backup Hyper-V,
- Backup VMware,
- Backup VMware dla darmowych licencji,
- Windows Operating System Backup – VHD,
- Backup z wykorzystaniem skryptów pre i post,
- Backup obrazu dysku,
- Harmonogramy backupów,
- Backup otwartych plików (VSS),
- Filtr plików oraz folderów,
- Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),
- Wyłączanie komputera po wykonaniu backupu,
- Backup na prawach użytkownika systemu Windows,
- Backup na prawach użytkownika AD,
- Przywracanie danych do wskazanego katalogu,
- Przywracanie danych do pierwotnej lokalizacji,
- Przywracanie wybranej wersji pliku,
- Możliwość backup-u z wykorzystaniem wielu rdzeni procesora,
- Możliwość przywracania z wykorzystaniem wielu rdzeni procesora,
- Przywracanie plików z określonego hosta,
- Przywracanie plików z określonego projektu,
- Przywracanie całych systemów operacyjnych,
- Przywracanie Exchange bezpośrednio do serwera.
- Przywracanie Hyper-V bezpośrednio do hosta maszyn,
- Przywracanie Exchange 2013 na poziomie pojedynczej skrzynki,
- Usuwanie plików przesłanych jako backup,
- Usuwanie wybranej wersji pliku,
- Wyszukiwanie plików w repozytorium użytkownika,
- Nadpisywanie plików podczas ich przywracania.

Synchronizacja

Funkcjonalność synchronizacji w aplikacji klienckiej umożliwia automatyczne przesyłanie plików z wybranego katalogu na serwer backupu oraz pobieranie plików przesłanych przez inne

urządzenia w ramach konta użytkownika. W jej skład wchodzą:

- Synchronizacja wybranego katalogu,
- Wstrzymywanie oraz wznawianie synchronizacji,
- Zmiana katalogu synchronizowanego,
- Lista synchronizowanych plików,
- Wyłączanie synchronizacji,
- Szyfrowanie synchronizowanych plików.

Magazyn

Dane przechowywane są w minimum 2 profesjonalnych, certyfikowanych DataCenter na terenie Polski, oddalonych od siebie o minimum 300km

Ustawienia

Użytkownik końcowy może konfigurować zainstalowaną aplikację w następującym zakresie:

- Zmiana języka aplikacji,
- Automatyczne logowanie,
- Zapamiętywanie danych logowania,
- Automatyczne uruchamianie programu przy starcie systemu,
- Eksport oraz import konfiguracji do pliku,
- Eksport oraz import konfiguracji na serwer,
- Ograniczenie ilości przechowywanych wersji,
- Ustawianie priorytetu dla procesu backupu,
- Zmiana klucza szyfrującego,
- Ustawienia proxy,
- Ustawienia przepustowości/zajętości pasma,
- Konfiguracja wydajności procesu backupu,
- Możliwość ograniczenia obciążenia dysku twardego,
- Możliwość wyłączenia zdalnego zarządzania.

Aktualizacje

Aplikacja kliencka może być aktualizowana na 2 sposoby:

- Automatycznie,
- Ręcznie

Bezpieczeństwo

Następujące funkcje odpowiedzialne są za bezpieczeństwo plików przesyłanych plików za pośrednictwem aplikacji klienckiej:

- Zastąpienie nazwy pliku GUID-em,
- Szyfrowanie danych algorytmem AES 256 CBC zawsze po stronie komputera użytkownika,
- Kompresja danych,
- Transmisja po bezpiecznym protokole SSL,
- Deklaracja domyślnego klucza szyfrującego,
- Deklaracja klucza szyfrującego użytkownika,
- Zmiana klucza szyfrującego,
- Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,
- Obliczanie sumy kontrolnej SHA-1,

Obsługiwane języki

- polski
- angielski

Pozostałe

- Shell Menu (menu kontekstowe systemu Windows),
- Kreator pierwszego uruchomienia,
- Rozbudowanie logi aplikacji kliencie oraz usługi,
- Możliwość Instalacji samej usługi – do zarządzania przez Management Center,
- Komunikaty z tray,
- Wskazywanie statusu połączenia z serwerem,
- Mechanizm łatwego raportowania błędów.

APLIKACJA CLI

Aplikacja CLI jest aplikacją JAVA obsługiwaną z linii komend. Powinna posiadać silnik backupu spójny z silnikiem backupu aplikacji Windows przez co proces backupu realizowany jest w jednakowy sposób.

- Jedynie backup plikowy
- Wbudowana pomoc

CENTRALNE ZARZĄDZANIE

- Zdalne zarządzanie aplikacjami klienckimi,
- Tworzenie i edycja użytkowników,
- Zdalne tworzenie zadań backupu,
- Wyzwalanie backupów na aplikacjach klienckich,
- Edycja projektów backupów zapisanych na urządzeniach końcowych,
- Przywracanie danych, które zostały poddane backupowi, na urządzenie użytkownika,
- Zdalna konfiguracja utylizacji zasobów komputera klienckiego przez aplikacje podczas wykonywania backupu,
- Wgląd do dziennika zdarzeń poszczególnych użytkowników platformy,
- Grupowanie projektów w szablony,
- Zarządzanie szablonami backupów,
- Przesyłanie zdefiniowanych szablonów do aplikacji klienckich,
- Zarządzanie sesjami backupu,
- Zdalna i cicha instalacja,
- Pobieranie informacji na temat urządzeń użytkowników aplikacji klienckich,
- Pobieranie aplikacji klienckich,
- Możliwość raportowania błędów,
- Generowanie raportów oraz wykresów,
- Zarządzanie szablonami backupu,
- Monitorowanie sesji,
- Dodawanie nowych oraz edycja istniejących klientów,
- Przegląd stanu licencji,
- Wykresy oraz statystyki,
- Wskazywanie statusu połączenia z serwerem,

APLIKACJE MOBILNE

Cechy wspólne

- Pobieranie danych przesłanych na magazyn chmurowy w formie backupu,
- Pobieranie danych przesłanych do *Aktówki*,
- Wysyłanie danych do *Aktówki*,
- Listowanie przesłanych plików,
- Współdzielenie plików znajdujących się w przestrzeni *Aktówki*,

- Generowanie linków publicznych dla plików znajdujących się w *Aktówce*,
- Szyfrowanie danych na urządzeniu przed wysyłką na serwery,
- Deszyfrowanie danych po stronie urządzenia,
- Szyfrowanie transmisji przy użyciu protokołu SSL,
- Dostęp do dziennika zdarzeń,
- Backup i przywracanie jedynie po WiFi,
- Wiele wersji językowych.

Android

- Definicję klucza szyfrującego,
- Kreator pierwszego uruchomienia,
- Backup kontaktów,
- Backup plików,
- Backup wiadomości SMS oraz MMS,
- Backup multimediów,
- Szczegółowe logi aplikacji,

iOS

- Backup kontaktów,
- Backup kalendarza,
- Backup multimediów,
- Filtr plików pobranych,
- Czyszczenie repozytorium pobranych plików,

PANEL WEB DLA UŻYTKOWNIKA

- Włączanie/wyłączanie aktówki,
- Zarządzanie użytkownikami w ramach licencji,
- Ustawianie klucza szyfrującego,
- Reset klucza szyfrującego,
- Usuwanie hostów,
- Wyświetlanie oraz pobieranie plików przesłanych jako backup,
- Wyświetlanie oraz pobieranie plików z przestrzeni *Aktówki*,
- Wysyłanie plików do *Aktówki*,
- Kopiowanie oraz przenoszenie plików w obrębie *Aktówki*,
- Przed wysyłką do *Aktówki* pliki są szyfrowane na urządzeniu użytkownika,

- Bezpieczna transmisja za pośrednictwem protokołu SSL,
- Tworzenie linków publicznych dla plików znajdujących się w *Aktówce*,
- Możliwość definiowania ważności linku,
- Możliwość zmiany ważności linku,
- Możliwość wysłania linku mailem bezpośrednio z panelu,
- Możliwość zarządzania linkami,
- Tworzenie katalogów w przestrzeni *Aktówki*,
- Współdzielenie plików z *Aktówki*,
- Możliwość wyboru użytkowników do współdzielenia z listy,
- Możliwość zarządzania zasobami współdzielonymi,
- Możliwość wysłania zaproszenia do systemu,
- Usuwanie plików z przestrzeni *Aktówki,*
- Dostęp do dziennika zdarzeń,
- Konfiguracja powiadomień mailowych,
- Zmiana oraz reset hasła użytkownika,
- Rozróżnianie typu urządzeń z którego pochodzi backup,
- Zarządzanie licencją– Modyfikacja, przedłużenie.
- Zarządzanie podziałem przestrzeni pomiędzy użytkownikami.

ARCHITEKTURA SYSTEMU

- Architektura Klient- - Serwer,
- Aplikacje klienckie wyposażone w mechanizm wydajnego cache,
- Możliwość pełnej redundancji elementów systemu,

WSPIERANE SYSTEMY OPERACYJNE

- Microsoft Windows 7 i nowsze
- Microsoft Windows Server 2008 R2 i nowsze
- Unix/Linux,
- OS X,
- Novell NetWare 6.5.
- Android
- iOS

Licencjonowanie

- Licencja subskrypcyjna, obowiązująca przez okres trwania Programu, tj. do 30.06.2026 r.

- Licencjonowanie nie ogranicza ilości zabezpieczanych stacji - jedynym limitem jest zajętość magazynu

● **Magazyn chmurowy powinien mieć pojemność minimum 500 GB**

b) Zakup i wdrożenie sieciowego serwera plików do archiwizacji danych dla Urzędu Miejskiego w Pyzdrach

Procesor	Procesor osiągający w teście PassMark CPU Average CPU Mark Multithread Rating co najmniej 4600 punktów w kategorii CPU Mark. Wynik dostępny na stronie: https://www.cpubenchmark.net/cpu_list.php ("lub równoważny")
Wbudowana pamięć RAM	min.4 GB
Maks. wielkość pamięci	32 GB
Rodzaj pamięci	SODIMM DDR4
Liczba obsadzonych gniazd pamięci	4
Liczba wolnych gniazd pamięci	0
Liczba wszystkich gniazd pamięci	4
Liczba zainstalowanych dysków	8
Dane techniczne dysków:	Typ dysku HDD Typ napędu Wewnętrzny Pojemność dysku 10 TB Interfejs dysku SATA III - 6 Gb/s Prędkość obrotowa 7200 obr/min Bufor 256 MB Okres gwarancji (miesiące) 36 Dyski wzmocnione poprzez technologię AgileArray i czujniki wibracji Dysk przeznaczony do serwerów NAS

	Waga max 650 g Wysokość max.26.11 mm Szerokość max.101.85 mm Głębokość max.146.99 mm
Maks. liczba dysków	8
Interfejs dysku	SATA
Obsługa hot-swap dysków	Nie
RAID	Tak
Poziomy RAID	• 0 • 1 • 10 (1+0) • 5 • 6 • JBOD
Protokoły sieciowe	• SMB, • AFP, • NFS, • FTP, • WebDAV, • CalDAV, • iSCSI, • Telnet, • SSH, • SNMP, • VPN (PPTP, OpenVPN, L2TP).
Architektura sieci	GigabitEthernet
Interfejs sieciowy	4 x 10/100/1000 Mbit/s
Gniazda we/wy	• 1 x eSATA • 4 x RJ-45 LAN • 2 x USB 3.0
Liczba wentylatorów	Min. 2
Wentylator	8 cm
Obudowa	Rack 2U

Gniazda rozszerzeń	1 x PCIe 3.0 x 8
Zasilanie	• 100 - 240 V (prąd zmienny) • 50 / 60 Hz, jednofazowo
Akcesoria w zestawie	• Przewodnik szybkiej instalacji • Pakiet akcesoriów • Przewody zasilania prądem przemiennym (RS1221RP+) x2 /1 zwykły przewód i 1 przewód C13 do C14 (RS1221+)
Waga	8.4 kg
Wymiary	max.88 × max.482 × max.407,5 mm
Pozostałe parametry	Wspornik do montażu szafy: Szafa typu rack 19" z 4 słupkami
Kryteria oceny równoważności	Wszystkie wymienione powyżej parametry, wymagania, określenia należy traktować jako minimalne. Zamawiający dopuszcza zastosowanie innych niż wymienione pod warunkiem, że będą lepsze niż określone w niniejszej tabeli. Wykonawca w przypadku zaoferowania rozwiązań równoważnych zobowiązany jest do wykazania, że są one lepsze niż te opisane przez Zamawiającego. Zamawiający uzna za równoważne rozwiązania, które będą lepsze niż minimum określone przez Zamawiającego, np. większa ilość pamięci RAM, większa pojemność dysków, więcej portów USB, więcej certyfikatów jakości itp. Itd.

c) Zakup i wdrożenie sieciowego serwera plików archiwizacji danych dla Miejsko - Gminnego Ośrodka Pomocy Społecznej w Pyzdrach.

Procesor	Procesor osiągający w teście PassMark Performance Test, co najmniej 2940 punktów w kategorii CPU Mark. Wynik dostępny na stronie: https://www.cpubenchmark.net/cpu_list.php ("lub równoważny")
Wbudowana pamięć RAM	min.2 GB
Maks. wielkość pamięci	6 GB
Rodzaj pamięci	SODIMM DDR4
Liczba obsadzonych gniazd pamięci	1
Liczba wolnych gniazd pamięci	0
Liczba wszystkich gniazd pamięci	1
Liczba zainstalowanych dysków	4
Dane techniczne dysków:	Pojemność: 8000 GB Format: 3.5 " Interfejs SATA: 6Gb Prędkość obrotowa: 7200 rpm Bufor: 256 MB Średni czas dostępu: 8.5 ms Wytrzymałość (praca): 70 G Wytrzymałość (spoczynek): 250 G MTBF: 1000000 h Temperatura pracy: 0-60 st. C NCQ: TAK Zapis prostopadły: TAK Pobór prądu (spoczynek): max. 7,2 W Pobór prądu (praca): max.9 W Głośność: max.27 dB Wymiary: max.147 x max.101,60 x max.26,11 Waga: max. 780 g Informacje dodatkowe: 3 lata gwarancji. Dysk przeznaczony do serwerów NAS. Czujnik wibracji RV.

Maks. liczba dysków	4
Obsługa hot-swap dysków	Tak
RAID	Tak
Poziomy RAID	• 0 • 1 • 10 (1+0) • 5 • 6 • JBOD
Protokoły sieciowe	• SMB1 (CIFS) • SMB2 • SMB3 • NFSv3 • NFSv4 • NFSv4.1 • NFS Kerberized sessions • iSCSI • HTTP • HTTPs • FTP • SNMP • LDAP • CalDAV
Architektura sieci	GigabitEthernet
Interfejs sieciowy	2 x 10/100/1000 Mbit/s
Gniazda rozszerzeń	min. 2 x M.2
Gniazda we/wy	• min.2 x RJ-45 LAN • min.2 x USB 3.0
Liczba wentylatorów	2
Wentylator	9.2 cm
Obudowa	Tower
Zasilanie	• Zasilacz: 90 W • Napięcie wejściowe zasilania prądem zmiennym: 100V to 240V AC • Częstotliwość zasilania: 50/60 Hz, Jednofazowy

	• Zużycie energii: 28.3 W (dostęp); 8.45 W (hibernacja dysków twardych)
Akcesoria w zestawie	• Jednostka główna • Pakiet akcesoriów • Zasilacz • Kabel zasilania • 2 x Kabel LAN RJ-45 • Przewodnik szybkiej instalacji
Waga	max.2.18 kg
Wymiary	max.166 x max.199 x max.223 mm
Kryteria oceny równoważności	Wszystkie wymienione powyżej parametry, wymagania, określenia należy traktować jako minimalne. Zamawiający dopuszcza zastosowanie innych niż wymienione pod warunkiem, że będą lepsze niż określone w niniejszej tabeli. Wykonawca w przypadku zaoferowania rozwiązań równoważnych zobowiązany jest do wykazania, że są one lepsze niż te opisane przez Zamawiającego. Zamawiający uzna za równoważne rozwiązania, które będą lepsze niż minimum określone przez Zamawiającego, np. większa ilość pamięci RAM, większa pojemność dysków, więcej portów USB, więcej certyfikatów jakości itp. Itd.